SOUTH CAROLINA TRUSTWORTHY INFORMATION SYSTEMS HANDBOOK

TABLE OF CONTENTS

Appendices

A1 Glossary
Defines terms that are used throughout the *Handbook*

A2 Bibliography
Provides citations to works consulted during *Handbook* development

A3 Citation
Citation of the *Trustworthy Information Systems Handbook*

A4 Background Information
Background of the Trustworthy Information Systems Project

A5 Methodology
Trustworthy Information Systems Project Methodology

A6 South Carolina Laws and Policies
South Carolina Laws and Policies Relating to Electronic Records

A7 Legal Issues
Legal Issues Affecting Electronic Records Management

PART 1: Introduction[1]

1.1: Why is a trustworthy information system important?

Records and information in government are extremely important for the following reasons:

- They facilitate government business
- They demonstrate government accountability
- They serve as evidence of government activity in South Carolina for current and future users of government information

In the face of the rapid growth of information technology, government information systems must demonstrate accountability through sound information management and documentation of government activity. Increasingly, attorneys are making electronic evidence a central focus of litigation. Courts, too, are paying attention and recognizing that electronic data means more than obtaining a printout of computer files. For instance, the Federal Code of Civil Procedure requires litigants to disclose categories and locations of relevant electronic files early in the litigation process or risk the possibility of an on-site search of their computer system. As a result of our evolving legal environment, you are required to maintain accurate electronic files and any destruction of data must be scheduled and carried out in a timely manner. Failure to properly plan or care for electronic data and records could make it harder to find and produce legally admissible records when required by law.

You can lessen the likelihood for problems through practical measures. At a minimum, you should know what information your system holds and how you can find it quickly and cost effectively. Additionally, you must also take steps to prove to the court that you have established and strictly followed well-documented procedures that prevent unauthorized access to your files and that the systems you manage provide timely and accurate information.

Producing trustworthy information is an attainable goal that should be an objective of every system manager. The following handbook is designed to assist you in creating and maintaining trustworthy information systems. We have developed this handbook to encourage you to practice good records management within an automated environment. They can help you, as a state or local government agency manager, produce records that meet everybody's needs — yours, the court's, the auditor's, and any other legitimate record user's. This handbook can be used for evaluating the trustworthiness of any government information system — large or small, old or new. It provides a valuable set of proven tools that your agency can apply, practically and efficiently. We encourage you to make this handbook your own!

---

[1] This handbook is adapted from the *Trustworthy Information Systems Handbook*, Version 4, July 2002, written and published by the Minnesota State Archives [www.mnhs.org/preserve/records/tis/tis.html]. It also references the international standard *ISO 15489-2*, First Edition, 2001-09-15.

1.2: What is a trustworthy information system?

Trustworthiness refers to an information system's accountability and its ability to produce reliable and authentic information and records.

We use the words authenticity, reliability and integrity when we talk about the information and records that the information system creates. Understanding these concepts is key to developing a trustworthy information system.

Authenticity
Authenticity simply means a record is what it purports to be. An authentic record is one that can be proven.

a) to be what it purports to be,
b) to have been created or sent by the person purported to have created it or sent it, and
c) to have been created or sent at the time purported

Reliability
Reliability refers to the authority and trustworthiness of records as evidence — their ability to stand for the facts.

a) A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

Unfortunately, a record can be authentic but not reliable. An authentic record will not be considered reliable when, over time, some part of its content, structure or context has been lost.

Integrity
The integrity of a record refers to its being complete and unaltered. If your records management policy allows for changes to a record after it is created, strict control of this process must be maintained. This includes specifying who is allowed to make any additions, deletions or annotations and under what circumstances. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

With electronic records and information in digital formats, we cannot demonstrate reliability, authenticity and integrity as easily as we can with paper records. We cannot see, touch, or examine electronic records in any intelligible way without the assistance of hardware and software. The computer, unlike a human being, does not bear accountability for itself; people in government make information systems accountable. It follows, then, that in building information systems, we need to establish and create procedures, system documentation, and descriptions of system information as a means to make the system accountable. This handbook provides the next best thing — the tools needed to examine government information systems for trustworthiness

1.3: What is the process for establishing trustworthiness?

Establishing the trustworthiness of an information system typically takes several steps and requires the collaboration of people with a variety of skills and knowledge. The Handbook's structure parallels the process and guides the reader along. Part 1, which you are reading now, provides background to help you get started. Parts 2 and 3 contain the criteria sets and checklists to help you evaluate your systems. Those undertaking the examination process for the first time are strongly encouraged to read through the entire handbook completely before beginning their project. Each successive step in the process builds on those before and it is important that none be slighted or skipped. The proper establishment of the trustworthiness of an information system depends on the completeness of the examination process.

Step 1: Assemble team ***(Section 1.4: "Who should participate?")***

Step 2: Choose a criteria selection method ***(Section 1.5 "How do you apply the trustworthy information systems criteria" & 1.6: "When can you apply the trustworthy information systems criteria?)***

Step 3: Determine the importance of the information in the system ***(Section 1.7: "How important is your information?")***

Step 4: Document the process ***(Section 1.8: "Why are metadata and documentation important?")***

Step 5: Select appropriate criteria ***(Section 2.1: "What are the criteria for a trustworthy information system?")***

Step 6: Implement and document choices ***(Section 1.8: "Why are metadata and documentation important?")***

1.4: Who should participate?

The *Handbook* encourages collaboration among a variety of people with diverse sets of skills and expertise. They are valuable assets in reaching your goal of information system trustworthiness.

Ideally, teams of agency personnel with a range of skills and knowledge will work together in this process. Your team should include people who have:

- Knowledge of agency and local government business, policy, and procedures. They know which laws and policies apply to your agency's information. Agency attorneys and auditors are valuable in this area.
- Knowledge of information access and data practices. They know who can access the information and for what reasons, and how long information needs to remain accessible. Agency records managers and the South Carolina Department of Archives and History can help in the process.
- Skills in computing, information technology, and information systems design. They can provide advice and propose options on what technologies and methodologies would work to accomplish business needs. Your information systems and technology staff, and even selected vendors, should be able to provide answers to questions.

The team should first be educated and made aware of the importance of information system trustworthiness and why the evaluation process is necessary. The team also needs to know the value of documenting their decisions, and they should be kept appraised of progress while system development is underway.

With a diverse and knowledgeable team assembled, you are on the right track for establishing information system trustworthiness.

1.5: How do you apply the trustworthy information systems criteria?

The Trustworthy Information Systems (TIS) criteria can be used in many ways depending on your agency's particular situation. Use of the criteria varies depending on a number of agency-specific factors such as:

- Agency information needs and policies
- Information system size, type, and scope
- Phase of information system development life cycle
- Agency size, staff, and procedures

The TIS criteria set presents itself much like a cafeteria line, with a wide array of criteria choices in different categories. The costs for implementing any of the criteria vary. If you think about a cafeteria line, customers make choices based on their hunger, dietary needs, and budgets.

In the TIS criteria cafeteria line, agency information system development teams face similar choices:

- What criteria items do we absolutely need to do our business and to meet information requirements?
- Which ones would be nice to have?
- What are the costs of implementing selected criteria?
- What are the costs (up-front and hidden) associated with not implementing them?

Agencies have different information needs and operate under different policy mandates and statutes. What's important to one agency may have little relevance to another. Therefore, the choices you make should represent what is appropriate for your organization and the individual information system(s).

1.6: When can you apply the trustworthy information systems criteria?

You can use the *Handbook* at any time during information system development. It is never too late to think about system trustworthiness. However, the earlier during the system development life cycle that you consider its trustworthiness, the better off you'll be.

Option 1: Applying the handbook during system design and development

During the analysis phase of system development, before a lot of time and money is spent on system design, is the most opportune time to weigh all of the TIS criteria that might be important to implement. At this time, you can think about the big picture without the constraints of a system that's already well along in development or operation. The steps in this instance are as follows:

1) Determine the value of your data
2) Weigh that value against the costs (time, money, etc.) of implementing each criteria
3) Choose only those criteria that support your determined level of risk
4) Implement
5) Document your choices (including handbook version, refer to Appendix A) and actions
6) Reassess needs and risks on a regular basis

Option 2: Applying the handbook to an existing information system

Obviously, establishing the trustworthiness of an information system is a process most easily undertaken during the analysis/planning phase before the design is nailed down. That's the ideal, but most agencies don't have that luxury. The handbook is useful at any point during the system development life cycle and can be used to examine the trustworthiness of systems that are already in place — your legacy systems. You can document what you presently have and establish how well the system is set up to meet various requirements. The steps in this instance are as follows:

1) Determine the value of your data
2) Examine your system with reference to the criteria
3) Determine which are already in place
4) Ask whether your current system configuration offsets your risks
5) Choose additional criteria for implementation after weighing the costs
6) Implement
7) Document your choices (including handbook version) and actions
8) Reassess needs and risks on a regular basis

Information systems are not static; they must respond to changes all the time. Changes in software, hardware, platforms, means of communications, and growth occur rapidly and necessitate considering and revisiting the TIS criteria on a periodic basis. Documentation of what you presently have can serve as a check on how well the system is set up to meet your various requirements.

1.7: How important is your information?

Determining Value/Assessing Risk

Records and data are not all equally valuable. Therefore, not all information systems containing records will require the same security measures and levels of trustworthiness. In determining the value of your information, you may want to consider such things as:

- What records and data are essential to your performing your business functions?
- What data is of permanent and/or historical value to you and to others?

In addition to determining value, you should also explore the risks associated with your information system. Again, not all information systems are equal. Losing data in some systems presents little more than an inconvenience. "At-risk" systems have a greater potential for legal problems and are financial liabilities. In many ways, this handbook serves as a risk management tool to limit your liability, both financial and legal. Questions you may ask include:

- What laws and regulations apply to your data?
- What areas and records might lawyers and auditors target?
- What are your industry's standards for system security, data security, and records retention?

Use the risk worksheet to evaluate the value and risk associated with your records.

1.8: Why are metadata and documentation important?

Documentation and metadata serve as the fundamental foundation of any trustworthy information system, enabling proper data creation, storage, retrieval, use, modification, retention, and destruction.

Documentation has two meanings. On a broad level, it is the process of recording actions and decisions. On a system level, documentation is information about planning, development, specifications, implementation, modification, and maintenance of system components (hardware, software, networks, etc.). System documentation includes such things as policies, procedures, data models, user manuals, and program codes. Documentation capture is not a system process.

Metadata can be simply defined as "data about data." More specifically, metadata consists of a standardized structured format and controlled vocabulary which allows for the precise description of record content, location, and value. Metadata often includes items like file type, file name, creator name, date of creation. Metadata capture, whether automatic or manual, is a process built into the actual information system.

Documentation and metadata establish accountability for information systems, and accountability goes hand-in-hand with trustworthiness — the ability to produce reliable and authentic records.

From the very beginning of your examination process, no matter where in the information system development life cycle you start, you must make a conscious effort to keep documentation. Documentation gathered after the fact always carries the possibility of incorrectness and/or incompleteness. Begin by gathering such information as:

- System name, owner, life cycle phase, purpose, etc.
- Rationale for the examination process
- Names and functions of team members
- Dates

As the examination process moves along, collect other documentation as appropriate. For example:

- Which version of the *Handbook* was used?
- Which criteria were selected? Why?
- Which criteria were not selected? Why?
- What were the responses to the various additional considerations?
- Who is responsible for implementation of the chosen criteria and each piece of supporting documentation?
- When were your choices implemented?

At the end of your initial system examination, you should have a complete record of your process and the choices you made along the way. By following up with consistent application of your choices and by maintaining the currency of your documentation as you make changes and revisit the criteria set, you will not only have an effective management tool for your system's proper administration, you will have evidence of its trustworthiness.

Bear in mind: complete documentation of an entire system is a daunting task that may not always be necessary for your particular situation — perhaps only certain functions need the careful attention outlined above. The value of your records must be weighed against cost and risk. Use the chart on the next page to gauge the various risks associated with your records before starting Part 2.

WHAT RISKS DO YOUR RECORDS AND RECORDS KEEPING PRACTICES POSE FOR YOU?

Do you have a records management program in place?

Approved, detailed current retention schedules ⟷ No program

Do you document your record keeping systems and practices?

Current data models, data dictionaries, procedures ⟷ No documentation

Do your records have a high audit and/or legal value?

Never audited or sued ⟷ Routinely audited and subject to litigation

Do you have a plan to preserve your vital records in case of disaster?

Current, comprehensive plan ⟷ No plan

Do your records contain confidential and private data?

No — only public data ⟷ Yes — there are significant data practices and privacy concerns

Do citizens and journalists request access to your records?

Never ⟷ Routinely

Do your records have historic value?

No historic value ⟷ Significant value to historians and genealogists

Do you have system security procedures in place?

Fully documented trustworthy system ⟷ No correlation of security needs with statutory mandates

PART 2: Criteria for Trustworthy Information Systems

The following criteria outline the best available practices for implementing a trustworthy information system. The most appropriate practices for a particular system may comprise only a certain number of these. Agencies choose what is reasonable and practical depending on a variety of factors. The important point is to make, justify, and document your choices in order to ensure consistent application and your agency's accountability for its decisions.

QUESTIONS TO ASK

What laws and/or regulations (state and federal) apply to the data within your system?

What are your industry's standards for system security?

What are your industry's standards for data security?

What areas/records might lawyers target?

What areas/records might auditors target?

What data is of permanent/ historical value to you and/or to others?

The criteria range from system- to record-level and are categorized into five main groups:

- system documentation
- security measures
- audit trails
- disaster recovery plans
- record metadata

Each of these areas contain specific criteria as well as items for further consideration:

- *Did You Know* highlights items drawn from South Carolina government sources concerning information systems and records management.
- Points under *Consider This* expand upon the criteria.
- The left-hand sidebar offers general *Questions to Ask* while working with the criteria set; those opposite a particular criteria group are complementary to its issues.

The criteria set will be updated as necessary to reflect new information. Sources are listed in the Bibliography section of this handbook.

Criteria Group 1: *System administrators should maintain complete and current documentation of the entire system.*

1A. System documentation should include, but is not limited to:

1. hardware (procurement, installation, modifications, and maintenance)
2. software (procurement, installation, modifications, and maintenance)
3. communication networks (procurement, installation, modifications, and maintenance)

Did You Know:

▲". . . all governmental bodies, as defined in the procurement code, must develop, in coordination with the CIO, a master plan for information technology procurements. Subject to CIO approval of the master plan, acquisitions of information technology by governmental bodies shall be through the CIO's Information Technology Management Office." (South Carolina CIO website.) www.cio.sc.gov/cioContent.asp?pageID=205

4. interconnected systems
   a. list of interconnected systems (including the Internet)
   b. names of systems and unique identifiers
   c. owners
   d. names and titles of authorizing personnel
   e. dates of authorization
   f. types of interconnection
   g. indication of system of record
   h. sensitivity levels
   i. security mechanisms, security concerns, and personnel rules of behavior

Consider This:

▲System documentation, including specifications, program manuals, and user guides, should be covered in retention schedules, and retained for the longest retention time applicable to the records produced in accordance with the documents.

▲Unique names and identifiers should remain the same over the lifetime of the units to allow tracking.

▲When a system is installed at more than one site, steps should be taken to ensure that each site is running an appropriate, documented, up-to-date version of the authorized configuration.

QUESTIONS TO ASK

What is the agency and department responsible for the system?

What is the agency and department responsible for applications?

What is the name and contact information of the person(s) responsible for system administration?

What is the name and contact information of the person(s) responsible for system security?

Has a formal risk assessment of the system been completed? Date? Performed by? Methodology? Findings?

What is the system's unique identifier and/or common name?

If connected to external systems lacking commensurate security measures, what mitigation procedures are in place?

Were design reviews and system tests run prior to placing the system in production? Were the tests documented?

▲ Audit trails of hardware and software changes should be maintained such that earlier versions of the system can be reproduced on demand.

▲ A process should be implemented to ensure that no individual can make changes to the system without proper review and authorization.

1B. Policy and procedure documentation should include, but is not limited to:

1. programming conventions and procedures
2. development and testing activities, including tools

Consider This:

▲ Periodic functional tests should include anomalous as well as routine conditions, and be documented such that they can be repeated by any knowledgeable programmer.

QUESTIONS TO ASK

Is application software properly licensed for the number of copies in use?

3. applications and associated procedures such as methods of entering/accessing data, data modification, data duplication, data deletion, indexing techniques, and outputs
4. identification of when records become official

Consider This:

▲ The South Carolina Department of Archives and History works with state agencies and local governments to ensure the proper management of South Carolina's public records, and to identify and protect those of historical value. We provide training and advisory services to state and local government offices and conduct training classes. For more information go to: www.state.sc.us/scdah/statelcl.htm

5. record formats and codes
6. routine performance of system backups. Each backup should be documented with backups being appropriately labeled, stored in a secure, off-line, off-site location, and subjected to periodic integrity tests.
7. routine performance of quality assurance and control checks, as well as performance and reliability testing of hardware and software on a schedule established through consultation with the manufacturers

Consider This:

▲ Identification devices (e.g., security cards) should be included in periodic testing runs to ensure proper functioning and to verify the correctness of identifying information and system privilege levels.

What other systems might records be migrated to?

▲ Each type of storage medium used should undergo regular statistical sampling following established procedures outlining sampling methods, identification of data loss and corresponding causes, and the correction of identified problems.

8. migration of records to new systems and media as necessary. All record components should be managed as a unit throughout the transfer.
9. standard training for all users and personnel with access to equipment

Consider This:

▲ Users should sign statements agreeing to terms of use. Such a document should include guidelines for: user responsibilities and expected behavior, consequences of inconsistent behavior or non-compliance, remote access use, internet use, use of copyrighted works, unofficial use of resources, assignment and limitations of system privileges, and individual accountability.

Criteria Group 2: *System administrators should establish, document, and implement security measures.*

2A. User Identification / Authorization

QUESTIONS TO ASK

Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?

1. User identification and access procedures should be established and documented. Users should be authenticated prior to being granted access.
2. Each user should be assigned a unique identifier and password. Identifiers and passwords should not be used more than once within a system. Use of access scripts with embedded passwords should be limited and controlled.

Consider This:

▲ Upon successful log-in, users should be notified of date and time of last successful log-in, location of last log-in, and each unsuccessful log-in attempt on user identifier since last successful entry.

▲ Where identification codes in human-readable form are considered too great a security liability, other forms should be employed such as encoded security cards or biometric-based devices.

Is there a list of all internal and external user groups and the types of data created and/or accessed?

3. Password rules should include standard practices such as minimum password length, expiration dates, and a limited number of log-on attempts. System administrators should determine what level and frequency of log-on error constitutes a misuse problem which, in turn, would trigger the notification of security personnel.
4. Users should be restricted to only the level of access necessary to perform their job duties.

QUESTIONS TO ASK

What are the procedures for the destruction of controlled-access hard copies?

Who can invoke change mechanisms for object, process, and user security levels?

Who (creator, current owner, system administrator, etc.) can grant access permissions to a record after the record is created?

5. Permission to alter disposition/retention codes, and/or to create, modify, and delete records should be granted only to authorized users with proper clearance. Modification of record identifiers is not allowed.
6. Access to private keys for digital signatures should be limited to authorized individuals.
7. Lists of all current and past authorized users along with their privileges and responsibilities should be maintained. The current list should be reviewed on a regular schedule to ensure the timely removal of authorizations for former employees, and the adjustment of clearances for workers with new job duties.
8. Personnel duties and access restrictions should be arranged such that no individual with an interest in record content will be responsible for administering system security, quality controls, audits, or integrity-testing functions. No individual should have the ability to single-handedly compromise the system's security and operations.

2B. Internal System Security

1. Access to system documentation should be controlled and monitored.
2. Access to output and storage devices should be controlled and monitored.

Have all positions been reviewed with respect to appropriate security levels?

How is information purged from the system?

How is reuse of hardware, software, and storage media prevented?

3. Controls should be in place to ensure proper security levels of data when archiving, purging, or moving from system to system. Controls should be in place for the transportation or mailing of media or printed output.
4. Procedures should be implemented to ensure the complete sanitization and secure disposal of hardware, software, and storage media when outdated or supplanted by newer versions, units, etc. Documentation should include date, equipment identifiers, methods, and personnel names.
5. Insecurity-detection mechanisms should be constantly monitoring the system. Fail-safes and processes to minimize the failure of primary security measures should be in place at all times.
6. Security procedures and rules should be reviewed on a routine basis to maintain currency.

QUESTIONS TO ASK

Is there a help desk or group that offers advice and can respond to security incidents in a timely manner?

7. Measures should be in place to guard the system's physical security. Items to consider include:
   a. access to rooms with terminals, servers, wiring, backup media
   b. data interception
   c. mobile/portable units such as laptops
   d. structural integrity of building
   e. fire safety
   f. supporting services such as electricity, heat, air conditioning, water, sewage, etc.
8. Security administration personnel should undergo training to ensure full understanding of the security system's operation.

2C. External System Security

1. In cases of remote access to the system, especially through public telephone lines, additional security measures should be employed. Possible action could include the use of input device checks, caller identification checks (phone caller identification), callbacks, and security cards.
2. For records originating outside the system, the system should be capable of verifying their origin and integrity. At a minimum, the system should:
   a. verify the identity of the sender or source
   b. verify the integrity of, or detect errors in, the transmission or informational content of the record
   c. detect changes in the record since the time of its creation or the application of a digital signature
   d. detect any viruses or worms present

Criteria Group 3: *System administrators should establish audit trails that are maintained separately and independently from the operating system.*

QUESTIONS TO ASK

Who can access audit data? Alter? Delete? Add?

How can the audit logs be read? Who can do this?

What tools are available to output audit information? What are the formats? Who can do this?

3A. General characteristics of audit trails include:

1. Audit trail software and mechanisms should be subject to strict access controls and protected from unauthorized modification or circumvention.
2. Audit trails should be backed up onto removable media periodically to ensure minimal data loss in case of system failure.
3. System should automatically notify system administrators when audit storage media is nearing capacity and response should be documented. When the storage media containing the audit trail is physically removed from the system, the media should be physically secured as required by the highest sensitivity level of data it holds.

Consider This:

▲ If audit trails are encoded to conserve space, the decode mechanism must always accompany the data.

3B. A system should be in place to track password usage and changes. Recorded events and information should include:

1. user identifier
2. successful and unsuccessful log-ins
3. use of password changing procedures
4. user ID lock-out record
5. date
6. time
7. physical location

3C. A system should be in place to log and track users and their online actions. Audit information might include:

1. details of log-in (date, time, physical location, etc.)
2. creation of files/records
3. accessed file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/security level)
4. accessed device identifiers
5. software use
6. production of printed output
7. overriding of human-readable output markings (including overwrite of sensitivity label markings and turning off of labeling mechanisms) on printed output
8. output to storage devices

QUESTIONS TO ASK

How are audit logs protected?

3D. For each record, audit trails should log, at a minimum, the following information:

1. record identifier
2. user identifier
3. date
4. time
5. usage (e.g., creation, capture, retrieval, modification, deletion)

What mechanisms are available to designate which activities are audited? Who can do this?

Criteria Group 4: *System administrators should establish comprehensive disaster and security incident recovery plans.*

4A. Disaster and security incident recovery plans should be periodically reviewed for currency and tested for efficiency.

Did You Know:

▲"To protect the state's critical information technology infrastructure and associated data systems in the event of a major disaster, whether natural or otherwise, and to allow the services to the citizens of this State to continue in such an event, the Office of the State Chief Information Officer (CIO) should develop a Critical Information Technology Infrastructure Protection Plan devising policies and procedures to provide for the confidentiality, integrity, and availability of, and to allow for alternative and immediate on-line access to critical data and information systems including, but not limited to, health and human services, law enforcement, and related agency data necessary to provide critical information to citizens and ensure the protection of state employees as they carry out their disaster-related duties. All state agencies and political subdivisions of this State are directed to assist the Office of the State CIO in the collection of data required for this plan." (*South Carolina Code of Laws*. Protection of critical information technology infrastructure and data systems. 1-11-435. www.scstatehouse.org/code/t01c011.htm

4B. Security incident recovery plans.

1. Hazards include:
   a. hardware failure or malfunction
   b. software failure or malfunction
   c. network failure or malfunction
   d. human error
   e. unauthorized access and activity
2. Government agencies should contact the Office of the State CIO for assistance with incident-handling procedures and support.
3. Related resources include :
   a. CERT Coordination Center [www.cert.org]

4C. Disaster recovery plans.

1. Hazards include:
   a. fire and/or explosion
   b. water or flood
   c. wind or tornado
   d. lightning
   e. hurricane
   f. power outage
   g. insects
   h. rodents
   i. violence and/or terrorism
   j. human error
2. Government agencies should contact the South Carolina Emergency Management Division and review the "South Carolina Emergency Operations Plan"
   a. The South Carolina Emergency Management Division can assist with:
      1. risk assessments
      2. recovery strategy development
      3. plan development
      4. training
      5. plan test coordination
      6. plan maintenance
   b. Information regarding the South Carolina Emergency Management Division and its services is available at: [www.scemd.org]
3. Related resources include:
   a. South Carolina Department of Archives and History disaster preparedness and recovery guidelines available at: [www.state.sc.us/scdah/techlflt.htm]
   b. Federal Emergency Management Agency (FEMA) emergency response and recovery guidelines available at [www.fema.gov]

Criteria Group 5: *Each record and/or record series should have an associated set of metadata.*

QUESTIONS TO ASK

What are the components of a complete or final record of a transaction?

What are the minimum components necessary to provide evidence of a transaction? If you went to court, what would be the minimum information you would need?

Are there any laws, regulations, or professional best practices that specify the structure (including medium, format, relationships) of the record of a transaction or any of its components?

What information is necessary to interpret the contents of a record?

During which agency business processes might you have to access a record?

Who are the external secondary users of your records?

What are the rules, laws, and regulations that restrict or open access to these records to external secondary users?

What are the procedures for reproducing records for use by secondary users? What are the reproduction formats?

Is there a mechanism to indicate sensitivity level on hardcopies? Who can enable/ disable this function?

What are your industry's standards for records retention?

5A. This Recordkeeping Metadata Standard (developed by the state of Minnesota) includes twenty elements. Each is listed below along with associated sub-elements and the obligation for implementation.

1. **Agent** (**mandatory)
   Definition: An agency or organizational unit responsible for some action on or usage of a record. An individual who performs some action on a record, or who uses a record in some way.
   - 1.1 Agent Type (mandatory)
   - 1.2 Jurisdiction (mandatory)
   - 1.3 Entity Name (mandatory)
   - 1.4 Entity ID (optional)
   - 1.5 Person ID (optional)
   - 1.6 Personal Name (optional)
   - 1.7 Organization Unit (optional)
   - 1.8 Position Title (optional)
   - 1.9 Contact Details (optional)
   - 1.10 E-mail (optional)
   - 1.11 Digital Signature (optional)

2. **Rights Management** (**mandatory)
   Definition: Legislation, policies, and caveats which govern or restrict access to or use of records.
   - 2.1 MGDPA Classification (mandatory)
   - 2.2 Other Access Condition (optional)
   - 2.3 Usage Condition (optional)
   - 2.4 Encryption Details (optional)

3. **Title** (**mandatory)
   Definition: The names given to the record.
   - 3.1 Official Title (mandatory)
   - 3.2 Alternative Title (optional)

4. **Subject** (**mandatory)
   Definition: The subject matter or topic of a record.
   - 4.1 First Subject Term (mandatory)
   - 4.2 Enhanced Subject Term (optional)

5. **Description** (optional)
   Definition: An account, in free text prose, of the content and/or purpose of the record.

6. **Language** (optional)
   Definition: The language of the content of the record.

QUESTIONS TO ASK

What is the records disposition plan?

Who is responsible for authorizing the disposition of records?

Who is responsible for changes to the records disposition plan?

How does the system accommodate integration of records from other systems?

Who can access record metadata? Alter? Delete? Add?

SPECIAL QUESTIONS FOR DATA WAREHOUSES

Do you gather extraction metadata?

Do you cleanse the data? Do you document the procedure? Do you gather cleansing metadata?

Do you transform the metadata? Do you document the procedure? Do you gather transformation metadata?

What metadata and/or documentation do you offer users?

Who can access metadata? Alter? Delete? Add?

What are the legal liabilities regarding data ownership and custodial responsibilities? Where do data custody responsibilities reside — with the source systems, the warehouse system, or both?

Are there records retention schedules and policies for warehouse data? Is retention of warehouse data coordinated with retention for data extracted from the source systems?

7. **Relation** (optional)
   Definition: A link between one record and another, or between various aggregations of records. A link between a record and another information resource.
   7.1 Related Item ID (mandatory)
   7.2 Relation Type (mandatory)
   7.3 Relation Description (optional)

8. **Coverage** (optional)
   Definition: The jurisdictional, spatial, and/or temporal characteristics of the content of the record.
   8.1 Coverage Type (mandatory)
   8.2 Coverage Name (optional)

9. **Function** (optional)
   Definition: The general or agency-specific business function(s) and activities which are documented by the record.

10. **Date** (**mandatory)
    Definition: The dates and times at which such fundamental recordkeeping actions as the record's or records series' creation and transaction occur.
    10.1 Date/Time Created (mandatory)
    10.2 Other Date/Time (optional)

11. **Type** (optional)
    Definition: The recognized form or genre a record takes, which governs its internal structure.

12. **Aggregation Level** (**mandatory)
    Definition: The level at which the record(s) is/are being described and controlled. The level of aggregation of the unit of description (i.e., record or record series).

13. **Format** (optional)
    Definition: The logical form (content medium and data format) and physical form (storage medium and extent) of the record.
    13.1 Content Medium (mandatory)
    13.2 Data Format (mandatory)
    13.3 Storage Medium (mandatory)
    13.4 Extent (optional)

14. **Record Identifier** (**mandatory)
    Definition: A unique code for the record.

15. **Management History** (**mandatory)
    Definition: The dates and descriptions of all records management actions performed on a record from its registration into a recordkeeping system until its disposal.
    15.1 Event Date/Time (mandatory)
    15.2 Event Type (mandatory)
    15.3 Event Description (mandatory)

16. **Use History** (optional)
    Definition: The dates and descriptions of both legal and illegal attempts to access and use a record, from the time of its registration into a recordkeeping system until its disposal.
    16.1 Use Date/Time (mandatory)
    16.2 Use Type (mandatory)
    16.3 Use Description (optional)

17. **Preservation History** (optional)
    Definition: The dates and descriptions of all actions performed on a record after its registration into a recordkeeping system which ensure that the record remains readable (renderable) and accessible for as long as it has value to the agency and to the community at large.
    17.1 Action Date/Time (mandatory)
    17.2 Action Type (mandatory)
    17.3 Action Description (mandatory)
    17.4 Next Action (optional)
    17.5 Next Action Due Date (optional)

18. **Location** (**mandatory)
    Definition: The current (physical or system) location of the record. Details about the location where the record usually resides.
    18.1 Current Location (mandatory)
    18.2 Home Location Details (mandatory)
    18.3 Home Storage Details (mandatory)
    18.4 Recordkeeping System (optional)

19. **Disposal** (**mandatory)
    Definition: Information about policies and conditions which pertain to or control the authorized disposal of records. Information about the current retention schedule and disposal actions to which the record is subject.
    19.1 Retention Schedule (mandatory)
    19.2 Retention Period (mandatory)
    19.3 Disposal Action (mandatory)
    19.4 Disposal Due Date (mandatory)

20. **Mandate** (optional)
    Definition: A source of recordkeeping requirements. For example, a piece of legislation, formal directive, policy, standard, guideline, set of procedures, or community expectation which (explicitly or implicitly) imposes a requirement to create, keep, dispose of, or control access to and use of a record.
    20.1 Mandate Type (mandatory)
    20.2 Refers To (mandatory)
    20.3 Mandate Name (mandatory)
    20.4 Mandate Reference (optional)
    20.5 Requirement (optional)

Consider This:

▲ Where records are not individually authenitcated, record series metadata may include the name or title of the individual responsible for validating or confirming the data within the record series, and for confirming that the particular series was produced in accordance with standard procedures.